BY ORDER OF THE COMMANDER 45TH SPACE WING

45TH SPACE WING INSTRUCTION 33-204

26 JANUARY 2011

Communications and Information

COMMUNICATIONS SECURITY (COMSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 45 SCS/SCXSIC

Certified by: 45 SCS/CC
(Lt Col Daniel L. Steele)

Pages: 7

This wing instruction implements the Air Force Policy Directive (AFPD) 33-2, Information Assurance (IA) Program; Air Force Instruction (AFI) 33-200, Information Assurance (IA) Management); AFI 33-201V2, Communications Security (COMSEC) User Requirements; AFI 33-230, Information Assurance Assessment and Assistance Program and other applicable COMSEC and Information Assurance (IA) directives. This is the initial issuance of this publication. This instruction applies to all 45th Space Wing (45 SW) and mission partners, including government civilians and contractors under contract by organizations supported by the 45 SW COMSEC program on a full or part-time basis. By establishing IA policy specifically for use in the wing, it acts as an addendum to other IA instructions and directives. Refer questions on the content of this instruction to the Communications Security Manager, 45 SCS/SCXSIC, 494-5479 (DSN 854-5479). COMSEC AFIs will always take precedence should conflicts be encountered concerning the retention of records associated with the COMSEC account. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Form 847s from the field through Major Command (MAJCOM) publications/forms managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/afrims**/.

1. COMSEC Program.

1.1. Overview. COMSEC refers to measures and controls taken to deny unauthorized persons information derived from information systems of the United States Government related to national security and to ensure the authenticity of such information systems. COMSEC protection results from applying security measures (i.e., crypto security, transmission security and emission security) to communications and information systems generating, handling, storing, processing or using classified or sensitive government or government-derived information, the loss of which could adversely affect national security interests. It also includes applying physical security measures to COMSEC information or materials.

2. Unit COMSEC Responsible Officer (CRO) and Secure Voice Responsible Officer (SVRO) Appointment.

2.1. IAW AFI 33-201V2, when required, each organizational/unit commander will appoint in writing a primary and at least one alternate focal point for unit COMSEC and secure voice accounts. If a unit has a CRO and also requires an SVRO, it is strongly recommended the CRO also serve as the SVRO. A SVRO will be appointed if the unit has no additional COMSEC requirements or if the unit commander determines that the CRO and SVRO should be different individuals.

2.1.1. Dependent upon the mission of an organization and the amount of COMSEC material involved, the duties of a CRO or SVRO may be intense. Unit commanders must be cognizant of the additional duty workload assigned to personnel appointed as CROs and/or SVROs. COMSEC demands extensive attention to detail and there is little room for error. Workload leveling is strongly encouraged. The below formula is suggested as a tool to accomplish this.

2.1.2. Formalize a complete list of additional duties with primary and alternates assigned as appropriate.

2.1.3. Categorize each additional duty as level 1, 2 or 3 based on the time requirement it levies on the appointee (1 is lowest).

2.1.4. Ensure additional duties are assigned in such a way as to avoid more than one 3-level duty per individual.

2.1.5. Quantify each individual's time commitment to additional duties by summing the category number for each duty assigned.

2.1.6. Ensure additional duties are assigned in such a way as to avoid excessive duties for any one individual.

2.1.7. Unit commanders must appoint a new CRO or SVRO if the individual currently appointed as primary or alternate will be deployed or on temporary duty (TDY) for more than 90 days. This must be accomplished no later than 30 days prior to the individual’s departure.

2.1.8. If the primary CRO is being replaced he/she must accomplish an inventory of their COMSEC material with the newly appointed CRO. The managing COMSEC office will provide the CRO a current inventory of the unit's account to use in accomplishing this.

2.1.9. The departing CRO will complete the inventory with the newly appointed CRO before being relieved from the account. The newly appointed CRO will sign the inventory, post a copy in the account's six-part folder and provide a copy to the managing COMSEC office.

3. Training.

3.1. Training is mandatory for each newly appointed CRO and SVRO and annually thereafter. Training sessions are conducted on the second Tuesday of each month. Attendance will be confirmed no later than the last duty day before or the class may be cancelled. Personnel requiring training must make every effort to attend on the normally scheduled day. Individual training session's out-of-cycle will only be scheduled as a last alternative and coordinated through the trainee's unit commander. The COMSEC manager has the discretion to schedule any CRO or SVRO to attend if he/she feels additional training is required based on duty performance.

3.1.1. The COMSEC Manager will gauge comprehension of the training material by giving four tests at the end of key areas. Trainees are also required to perform several practical tests (i.e., accomplish/critique an AFCOMSEC Form 16, Disposition Record Card, SF 701, Activity Security Checklist, etc.). Responses are evaluated during the session to ensure a thorough understanding of the material before the trainee and trainer sign the AF Form 4168, COMSEC Responsible Officer and User Training Checklist.

3.1.2. Unit CROs and SVROs are required to train their users before granting access to COMSEC material and annually thereafter. CROs and SVROs will train their users to the level of training they received from the COMSEC office. Training material will be provided upon request.

3.1.3. The COMSEC Manager will conduct quarterly meetings with all CROs and SVROs to discuss error trends, new or updated procedures and any new developments in the COMSEC duties and responsibilities. Individuals can also take this opportunity to address any concerns or questions they may have.

4. Inspection Criterion.

4.1. IAW AFI 33-230, Information Assurance Assessment and Assistance Program, and this instruction, the 45 SW main and associated COMSEC subaccounts will be inspected using the following criteria.

4.1.1. Unit CROs and/or SVROs will accomplish a self-inspection, utilizing AF FM 4160, Information Assurance Assessment and Assistance Program (IAAP) Criteria, twice a year (January and July). The CRO/SVRO will forward the results to the managing COMSEC manager no later than the 21st day of the self-inspection month. The COMSEC manager will use these results as a comparison tool to any actual findings discovered during the routine semiannual inspection.

4.1.2. The managing COMSEC office will conduct a routine semiannual inspection of the local elements along with a 100% hands-on inventory of all COMSEC material in the February and August timeframe. A satisfactory or unsatisfactory rating is determined by the COMSEC manager based on the number and criticality of discrepancies.

4.1.3. The managing COMSEC office will conduct a minimum of two no-notice inspections of each local element annually. The frequency of no-notice inspections will be dependent on the number of deficiencies noted during previous inspection. For example, at least one no-notice inspection will be conducted according to Table 1.

Table 1. No Notice Inspection Criterion.

1 critical finding or 5-9 non-critical findings	within 3 months
2+ critical findings or 10+ non-critical findings	within 1 month

4.1.4. The managing COMSEC account and all local elements are subject to inspection by AFSPC/A6 biennially. All accounts and local elements are subject to inspection by AFSPC/IG and the Air Force Audit Agency (AFAA) at any time, provided inspectors or auditors meet the access requirements as defined in AFI 33-201V4.

4.1.5. The inspected unit commander and 45 SCS commander will be briefed on the results of each inspection. The 45 RMS commander will also be briefed on inspection results for Cape Canaveral AFS (CCAFS), Antigua Air Station (AAS) and Ascension Auxiliary Air Field (AAAF). If the account is managed by a contractor, the applicable government contract monitor will be briefed as well.

4.1.6. The final inspection report will be sent directly to the unit commander or government contract monitor for concurrence or non-concurrence and signature.

4.1.7. All reports will be routed to the 45 OG/CC for review. All unsatisfactory inspection results will be reported to the violating unit's group commander, 45 SW/CV and 45 SW/CC via the 45 OG/CC.

4.1.8. Local elements will respond to their managing COMSEC office on all inspection findings 10 days after receipt of initial report and every 30 days thereafter until the finding is closed, IAW AFI 33-230.

4.1.9. The managing COMSEC manager is the authority to close findings from the wing semiannual or no-notice inspection. AFSPC Inspector General (IG) or Air Force Audit Agency (AFAA) is the authority to close findings from their respective inspection.

5. Issuing COMSEC Material.

5.1. COMSEC material is issued to users no earlier than 10 days from the material's effective date. Users will be scheduled to pick up their material during a 2-day window in the 10-day period. Users will make every effort to meet their scheduled time for pickup.

6. Simple Key Loader (SKL).

6.1. All first time users of the SKL must complete the SKL Computer Based Training (CBT). A certificate of completion will be maintained in the account's six-part folder with the user's AF Form 4168.

6.2. The managing COMSEC office will establish the user's SKL account. The login ID will be the user's "first.last" name all lower case (e.g., john.doe). Variations will be used in the event of duplicate names.

7. Destruction.

7.1. For the first of the month routine destructions, users will make every effort to forward destruction reports to the COMSEC office before noon on the day of destruction. Users serviced by the Patrick AFB COMSEC account may FAX the destruction, SF 153, COMSEC Material Report, to 494-1317 or E-mail to: **45scs.ca623502@patrick.af.mil.**

7.2. If a user serviced by the Patrick AFB COMSEC account knows they will not be present on the first duty day for destruction, notify the COMSEC office by sending an E-mail to: **45scs.ca623502@patrick.af.mil.**

8. Secure Telephone Equipment (STE)/Bump-in-the-Line (BITL).

8.1. KSV-21 card(s) will be purchased by the user and ordered through the managing COMSEC office. Once the card(s) arrive, the managing COMSEC office will schedule a time for the CRO/SVRO to either bring their STE(s) to the office for keying or pick up the card(s). The COMSEC Manager will determine on a case-by-case basis which units can hold unassociated KSV-21 cards.

8.2. BITLs will be keyed by the managing COMSEC office and issued to the unit CRO/SVRO.

8.3. Each SVRO/CRO is required to register at the secure phone site to keep current with the latest product information and to obtain operating instructions for their secure voice devices: **https://www.iad.gov/securephone/index.cfm**.

9. Contact and Additional Information.

9.1. The PAFB COMSEC office can be contacted at (321) 494-5479 or DSN 854-5479, fax (321) 494-1317 or DSN 854-1317.

9.2. COMSEC support for CCAFS, Antigua AS and Ascension AAF is provided through a contract source. All questions or requests for support must be directed to the Eastern Range support contract program manager at commercial (321) 853-0890 or 6268, DSN 467-0890 or 6268.

9.3. Adopted Forms:

AF Form 847, *Recommendation for Change of Publication*

AFCOMSEC Form 16, *Safe Inventory*

AF Form 4160, *Information Assurance Assessment and Assistance Program (IAAP) Criteria*

AF Form 4168, COMSEC *Responsible Officer and User Training Checklist*

SF 153, COMSEC *Material Report*

SF 701, *Activity Security Checklist*

B. EDWIN WILSON, Brigadier General, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-2, Information Assurance (IA) Program, 19 April 2007

AFI 33-200, Information Assurance (IA) Management, 23 December 2008

AFI 33-201V1, Communications Security (COMSEC), 1 May 2005

AFI 33-201V2, Communications Security (COMSEC) User Requirements, 26 April 2005

AFI 33-201V4, Cryptographic Access Program, 15 April 2005

AFI 33-230, Information Assurance Assessment and Assistance Program, 4 August 2004

Abbreviations and Acronyms

45 SW—45th Space Wing

AAF—Auxiliary Air Field

AFAA—Air Force Audit Agency

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFSPC—Air Force Space Command

AS—Air Station

BITL—Bump-in-the-Line

CCAFS—Cape Canaveral Air Force Station

COMSEC—Communications Security

CRO—COMSEC Responsible Office

IA—Information Assurance

IAW—In Accordance With

IG—Inspector General

PAFB—Patrick Air Force Base

STE—Secure Telephone Equipment

SVRO—Secure Voice Responsible Officer